

Descarregamento de Tráfego de Redes IoT/Edge por Transmissões de Múltiplos Fluxos

Celso Ferreira da Silva^{1,2}
Aluno

Simone Ferlin³
Co-orientadora

Bruno Yuji Lino Kimura¹
Orientador

¹Universidade Federal de São Paulo, São José dos Campos - SP, Brasil

²TecSys do Brasil Industrial, São José dos Campos - SP, Brasil

³Ericsson AB, Estocolmo, Suécia

{celso.ferreira, bruno.kimura}@unifesp.br, simone.ferlin@ericsson.com

Resumo. *O conceito de um mundo totalmente conectado na tecnologia de quinta geração (5G) prevê a implementação massiva de pequenos e restritos dispositivos de Internet das Coisas (IoT). Nesses ambientes de IoT, as comunicações Máquina-a-Máquina (M2M) são essenciais para permitir que dispositivos (por exemplo, sensores, atuadores, medidores/monitores inteligentes) colem dados para um servidor remoto. Nesta dissertação, investigamos este cenário para propor, implementar e validar uma nova arquitetura para infraestruturas de IoT, mais eficiente, através do descarregamento de dados por transmissões de caminhos múltiplos na Internet. Os resultados experimentais do tráfego emulado por CoAP indicam que o nosso sistema proposto, juntamente com os benefícios do MPTCP, melhoram o desempenho das aplicações IoT. Mais especificamente, o descarregamento do tráfego de dados M2M baseado em múltiplos caminhos aumenta a vazão e reduz significativamente a latência das solicitações CoAP conforme o número de redes de sensores aumenta.*

Abstract. *The concept of a fully connected world in the fifth generation (5G) technology provides for the massive implementation of small and restricted Internet of Things (IoT) devices. In these IoT environments, such as Machine-to-Machine (M2M) communications are essential to allow devices (for example, sensors, actuators, smart meters/monitors) to collect data for a remote server. In this dissertation, we investigate this scenario to propose, implement and validate a new architecture for IoT infrastructures, more efficient, by downloading data through multipath transmissions on the Internet. The experimental results of the traffic emitted by CoAP indicate that our proposed system, together with the benefits of MPTCP, improve the performance of IoT applications. More specifically, offloading M2M data traffic based on multiple paths increases throughput and reduces the latency of CoAP requests as the number of sensor networks increases.*

1. Caracterização do Problema e Motivação

O paradigma de IoT tem possibilitado a criação de um amplo espaço de soluções tecnológicas para diversos domínios de aplicações, e.g., cidades inteligentes, energia inteligente, casas inteligentes, saúde inteligente, entre outros. A comunicação entre um grande número de dispositivos de baixo poder computacional e uma aplicação remota descreve

o principal modelo considerado nas mais diversas aplicações [Verma et al. 2016]. Tipicamente, em comunicações MTC (*Machine Type Communication*), dispositivos MTC mantêm conectividade com um servidor M2M remoto.

Em ambientes massivamente conectados em IoT, contudo, novos desafios são introduzidos, como [Hong et al. 2020]: requisitos de latência e *jitter* restritos de aplicações; custo elevado de escoamento de dados nos enlaces de saída (*uplinks*) de maior largura de banda; e o provimento de serviços ininterruptos. Para atacar estes desafios, este trabalho direciona esforços de investigação para o aprimoramento das arquiteturas e infraestruturas de IoT existentes através de métodos mais eficientes de comunicação M2M entre sensores e servidores remotos.

2. Objetivos, Contribuições e Subprodutos do Trabalho

Neste trabalho, os **objetivos** foram propor, implementar e validar uma nova arquitetura de comunicação M2M baseada em múltiplos caminhos (*multipath*) a partir de um novo elemento na rede IoT, o nó MPP (*MultiPath Proxy*), possibilitando descarregar o tráfego de um grande número de sensores sobre diferentes redes de acesso. Para tanto, construímos um sistema de acesso múltiplo de IoT como uma arquitetura de referência e avaliamos diferentes indicadores de desempenho de Camada de Transporte e seus impactos no descarregamento de tráfego M2M rumo a um servidor remoto. Como princípio de projeto, nesse sistema os sensores continuam inalterados, ou seja, dispositivos simples, de baixo custo e poder computacional, podendo ser conectados a um nó concentrador, o qual coleta e encaminha os dados dos sensores.

Diferente das arquiteturas existentes, nós conectamos o nó concentrador ao nó MPP. Implementamos um protótipo de um MPP leve, i.e., de baixo poder computacional, o qual é capaz de conectar a infraestrutura de IoT à Internet através de mais de dez redes de acesso, lidando de forma transparente com o tráfego de milhares de sensores. Para avaliar o desempenho da transmissão M2M, habilitamos conexões de caminhos múltiplos através do protocolo MPTCP (*MultiPath TCP*), RFC8684, junto ao MPP ligado a até três operadoras de redes 4G/LTE. Resultados experimentais com diferentes tamanhos de mensagens e números de sensores indicam redução drástica de latência, de 900 ms para 260 ms, e um aumento considerável de vazão em fluxos M2M para 4,000 (com duas redes de saída) e até 6,000 requisições/s (com três redes de saída), comparado as 1,600 requisições/s com uma única rede de saída.

As principais **contribuições** deste trabalho são:

- **Avanço no Estado da Arte.** Um nova arquitetura de comunicações M2M baseada em transmissões CMT (*Concurrent Multipath Transfer*) que melhora a eficiência do fluxo de dados de infraestruturas de IoT de conexões massivas.
- **Inovação Tecnológica.** Protótipo de um novo dispositivo de rede, o nó MPP, como elemento facilitador da implantação da arquitetura proposta.
- **Integração com Setor Produtivo.** Demonstração de viabilidade da arquitetura através de uma implementação como prova de conceito para fins de produção industrial (TecSys), com especial aplicação em monitoramento inteligente envolvendo grandes volumes de dados e dispositivos.

Como **subprodutos**, destacam-se: (1) a dissertação de mestrado [Silva 2020], (2) o protótipo do nó MPP e (3) a publicação resultante. A arquitetura proposta e a dis-

cussão de seus resultados aparecerão em artigo [Silva et al. 2021] aceito para publicação em abril de 2021 na revista *IEEE Communications Magazine*, um dos principais periódicos existentes na área de Redes de Computadores de elevado fator de impacto.

3. Trabalhos Relacionados

Através da agregação de redes de acesso fixo e móvel, as redes de acesso híbrido (*Hybrid Access Networks*) são alternativas viáveis para operadoras fornecerem serviços de acesso à Internet mais rápidos aos usuários. Em [Keukeleire et al. 2019], os autores apresentam protótipo de rede de acesso híbrido com o protocolo MPTCP. Um *proxy* HCPE (*Hybrid Customer Premises Equipment*) na rede de acesso é multiconectado com MPTCP a um *proxy* HAG (*Hybrid Access Gateway*) nas operadoras, permitindo transmissão CMT com a utilização simultânea de diferentes redes, como LTE e xDSL. Em [Liu et al. 2018], os autores propõem uma arquitetura também baseada em *proxies* MPTCP, denominada *MPTCP Tunnel*, para agregar a largura de banda com redes de acesso fixo e móvel. Em [Bocassini et al. 2013], os autores introduzem um novo gerenciador de caminhos para MPTCP, chamado *Binder*, que habilita transmissões CMT a partir de *gateways* distribuídos geograficamente em redes comunitárias. Em geral, esses trabalhos preveem soluções de redes de acesso híbrido para usuários finais através de *proxies* MPTCP, possibilitando que os usuários se beneficiem do transporte CMT de forma transparente, e.g., agregação de largura de banda, balanceamento de carga e tolerância à falhas. Diferentemente desses trabalhos, nesta dissertação propõe-se uma nova arquitetura de comunicação para infraestruturas de IoT/Edge, a qual habilita o suporte transparente ao CMT em transmissões M2M enquanto mantém intacto os sensores e as aplicações envolvidas, possibilitando ganhos significativos no escoamento eficiente de dados cenários de larga escala.

4. Resultados Obtidos

A seguir, discutimos os principais resultados obtidos.

4.1. Modelos de Comunicação de IoT

Normalmente, a comunicação M2M está relacionada a dois tipos principais de conectividade [Song et al. 2015]: entre um dispositivo MTC e um servidor M2M, ou entre dispositivos MTC. Neste trabalho, nós nos concentramos no primeiro tipo, em que a comunicação entre um grande número de sensores e uma aplicação remota descreve o modelo mais popular para várias aplicações M2M [Verma et al. 2016]. Segundo [Slabicki and Grochla 2016], o processamento, a comunicação e a sincronização entre os dispositivos MTC podem ser realizados em três níveis: (1) diretamente entre os dispositivos, (2) através de um roteador de acesso, (3) através do sistema remoto. No nível 1, os sensores e atuadores fazem parte da mesma rede de acesso. No nível 2, um roteador de acesso IoT multifuncional opera como um *proxy*, permitindo a comunicação entre dispositivos locais com o sistema remoto. No nível 3, a comunicação por meio do sistema remoto é responsável por coletar, processar dados e, eventualmente, responder aos sensores.

Neste trabalho, focamos no nível 3 e ilustramos na Figura 1 três modelos gerais de comunicação M2M para arquiteturas de IoT: dispositivo para servidor, concentrador para servidor, múltiplo acesso para servidor. Prevemos em cada caso até cinco componentes

principais: Domínio de Sensores (DS), Enlace de Acesso (L), Concentrador (C), MPP e servidor remoto (S), onde DS representa os sensores conectados a uma rede de um domínio de aplicação específica.

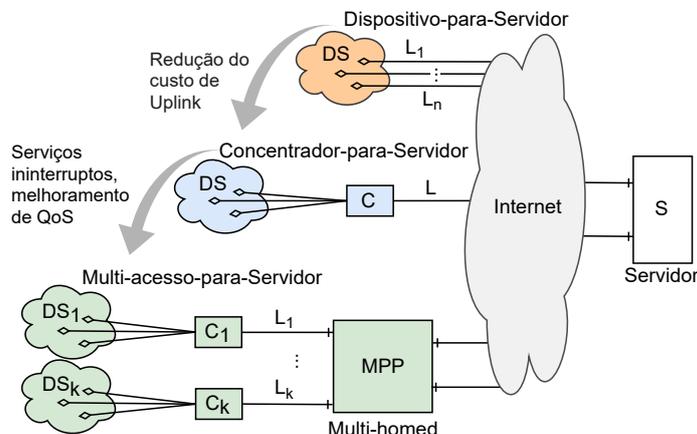


Figura 1. Modelos gerais de comunicação IoT/M2M [Silva et al. 2021].

4.2. Arquitetura Proposta

Para habilitar tráfego de múltiplos caminhos no modelo Multi-acesso-para-Servidor, propomos, implementamos e validamos um sistema fim-a-fim, cuja arquitetura é ilustrada na Figura 2. Entre DS e S, como parte do que descrevemos como *loop de controle* ① interno, temos o tráfego M2M. Consideramos aqui o tráfego de um protocolo típico de IoT, como o CoAP (*Constrained Application Protocol*), RFC7252. Enquanto MQTT (*Message Queuing Telemetry Transport*) prevê comunicação intermediada por *broker* em modelo *publish-subscribe*, o protocolo CoAP permite troca de mensagens em modelo REST/HTTP entre cliente e servidor, ou seja, mantém a semântica fim-a-fim entre sensores e servidores, além de prover mecanismos básicos controle de congestionamento. No meio, há o *loop de controle* ②, onde todo o tráfego M2M vindo de um domínio DS é encapsulado em uma única conexão TCP entre o nó concentrador C e um Servidor Proxy (SP). O nó C é responsável por agregar todos os dados de um ou mais DSs e encaminhá-los ao nó MPP. No *loop de controle externo* ③, os dados que chegam ao nó MPP são multiplexados em uma conexão de caminhos múltiplos. Em outras palavras, no *loop de controle* ③, a conexão de caminho único de *loop de controle* ② é multiplexada em até três sub-fluxos paralelos do MPTCP, aproveitando a agregação de vazão, latência reduzida e resiliência na transmissão com o nó SP remoto. No nó SP, os dados no *loop de controle* ③ são demultiplexados em uma única conexão, desagregados nas mensagens individuais CoAP e entregues ao nó S, onde o tráfego M2M atinge o servidor de aplicação.

Para implementarmos o *loop de controle* ①, foi utilizado a ferramenta *Californium CoAP Benchmark* (CoAPBench) [Kovatsch et al. 2014] nos nós C e S. A ferramenta emula o tráfego DS de diferentes aplicações IoT, gerando tráfego CoAP real de C para S. Com a execução do CoAPBench cliente e servidor em C e S, respectivamente, foi possível instanciar milhares de nós sensores CoAP sintéticos. Diferentes tamanhos de carga útil CoAP foram utilizados para avaliar o impacto do sistema implementado. Os dados em DS são coletados em C no *loop de controle* ② e são transportados por um túnel SSH (conexão TCP). Os fluxos CoAP/TCP se conectam diretamente através da porta SSH

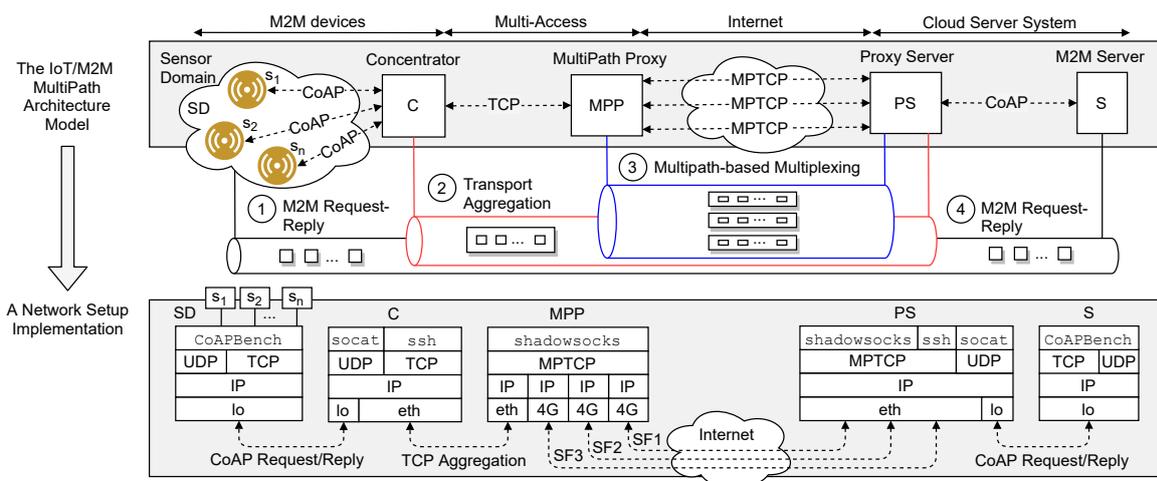


Figura 2. A arquitetura IoT/M2M de caminhos múltiplos: de um novo modelo de comunicação para uma implementação viável [Silva et al. 2021].

no nó C, porém os fluxos CoAP/UDP necessitam de um encapsulamento em segmentos TCP, o que é feito através da ferramenta *socat*. No *loop de controle* ③ é realizada a multiplexação de pacotes sobre os sub-fluxos paralelos do MPTCP, utilizando um *proxy socks5* implementado por *shadowsocks*. O principal componente da arquitetura está o *loop de controle* ③, que é o nó MPP, o qual foi prototipado em *System-On-a-Module* (SoM): CPU iMX6 Arm Cortex A7 Core 528 MHz, 512 MB de RAM e 64 GB de armazenamento SSD. O MPP possui um sistema Linux embarcado com MPTCP em sua última versão (v0.95) e o *proxy shadowsocks*. O Servidor Proxy (SP) é compatível com MPTCP e *shadowsocks*, onde se realiza a remontagem dos pacotes e encaminha para o servidor S.

4.3. Resultados Experimentais

Para validar e avaliar a arquitetura proposta, experimentos foram realizados na rede implementada a partir de emulações de fluxos CoAP com *CoAPBench*. Para tanto, configuramos a arquitetura proposta com dois (MPP-2P) e três caminhos (MPP-3P) de escoamento e comparamos os resultados com a solução padrão de caminho único (E2P-1P). Os experimentos incluíram um amplo conjunto de parâmetros para fluxos CoAP sobre UDP, CoAP sobre TCP, considerando a emulação de tráfego M2M com diferentes tamanhos de carga útil de requisições M2M, em diferentes escalas de redes de IoT. Particularmente, as cargas úteis dos pacotes CoAP foram de 4, 16 e 64 bytes e os tamanhos da rede de IoT foram de 250, 500, 1000 e 2000 sensores. Esse espaço de fatores e domínios de valores nos experimentos planejados possibilitou representar diferentes tipos de aplicações IoT, de redes pequenas às redes de larga escala.

As Figuras 3(a) e 3(b) mostram as vazões médias e os tempos médios de conclusão de requisição/resposta CoAP, respectivamente, para diferentes números de sensores, protocolos de transporte e número de caminhos de saída no nó MPP. Para fornecer uma visão geral do desempenho, esses resultados consideram todos os tamanhos de carga útil.

Com 250 sensores, o caminho único (E2E-1P) lida com quase toda a carga de tráfego. No cenário de 500 sensores, aumenta-se a taxa média de 2,000 requisições/s

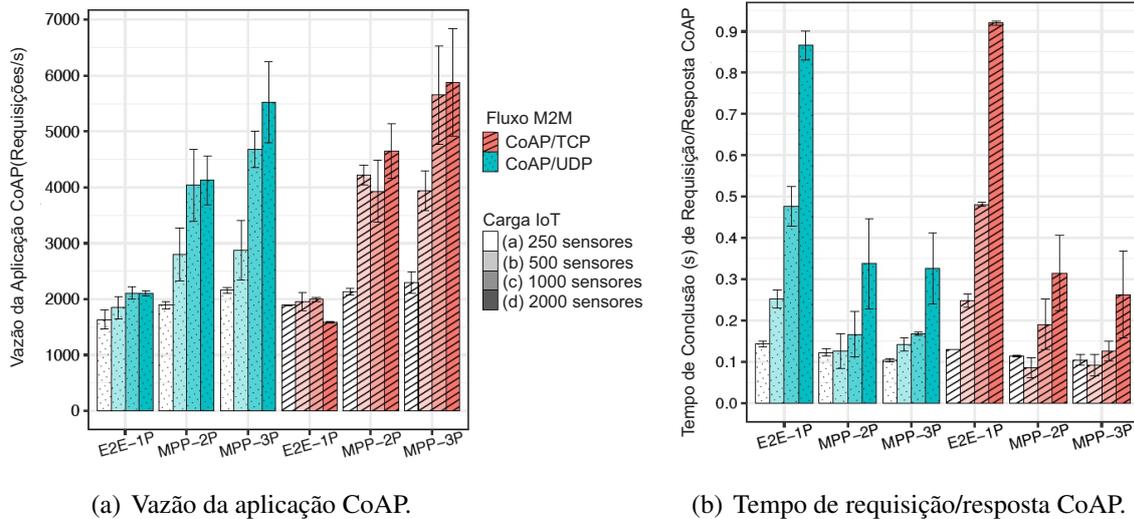
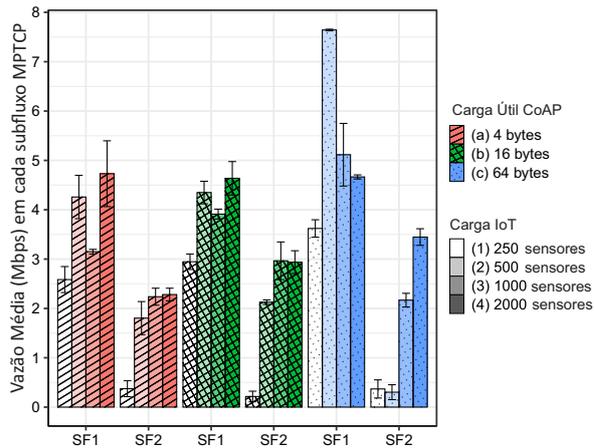


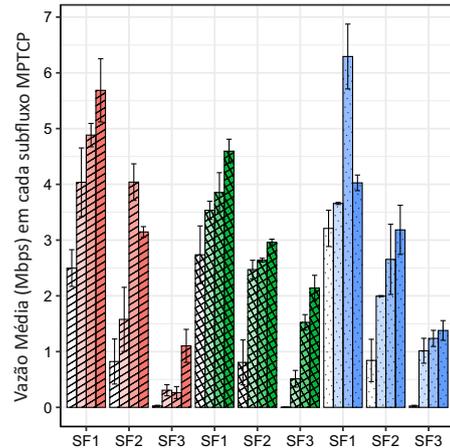
Figura 3. Resultados obtidos em transmissões M2M do protocolo CoAP na rede experimental implementada [Silva et al. 2021].

em E2E-1P para 4,000 requisições/s quando há dois caminhos (MPP-2P) disponíveis de descarregamento. Para 500 sensores, o tempo de conclusão é reduzido de 250 ms para 100 ms em média no caminho único (E2E-1P) e em dois caminhos (MPP-2P), respectivamente. No entanto, como a capacidade adicionada por um segundo caminho já acomoda a carga de tráfego para os 500 sensores, não há redução de latência com três caminhos (MPP-3P) de saída. Em vez disso, olhando para os cenários de 2,000 sensores, a adição de um segundo (MPP-2P) e um terceiro (MPP-3P) caminho aumenta a vazão de requisições para 4,500 e 5,900 requisições/s em média em comparação com 1,600 requisições/s em caminho único, mostrando assim o benefício da agregação do transporte por caminhos múltiplos. No entanto, mesmo com três caminhos (MPP-3P), não é possível sustentar toda a carga de tráfego de 2,000 sensores, fazendo com que a vazão atinja um limite, o que reflete no aumento das latências. Observamos que, à medida em que a carga de tráfego de sensores aumenta por trás do nó C, podemos melhorar substancialmente a transferência de dados CoAP fim-a-fim, em direção ao servidor S. Ao adicionar mais conexões entre os nós MPP e SP, ou seja, aumentando a capacidade de agregação e multiplexação por caminhos múltiplos, obtemos maior vazão de requisições/s e reduzimos os tempos de conclusão de requisição/resposta CoAP.

As Figuras 4(a) e 4(b) apresentam vazões do nó MPP com dois (MPP-2P) e três (MPP-3P) caminhos, considerando tamanhos de carga útil CoAP de 4, 16 e 64 bytes e cargas de 250, 500, 1000 e 2000 sensores. Os subfluxos MPP são indicados por SF1, SF2 e SF3 (para o cenário MPP-3P). Analisando os valores médios de RTT entre o MPP e o nó S, todas as redes (Claro, Tim e Vivo) apresentaram latências de aproximadamente 30 ms. No entanto, conforme mudamos a carga de tráfego, ou seja, aumentando de 250 para 2.000 sensores, os RTTs médios excederam 100 ms, o que interpretamos como um impacto de *buffering* na rede (*bufferbloat*). Aplicar a mesma carga de tráfego sobre subfluxos heterogêneos leva à degradação do desempenho, por exemplo, devido ao bloqueio (*head-of-line*). Por outro lado, o controle de congestionamento OLIA do protocolo MPTCP é capaz de equilibrar o congestionamento entre os subfluxos, enquanto os subfluxos mais



(a) Vazão do MPTCP com MPP-2P.



(b) Vazão do MPTCP com MPP-3P.

Figura 4. Vazão dos sub-fluxos em escoamento por dois e três caminhos disjuntos [Silva et al. 2021].

lentos têm menor prioridade com o escalonador de pacotes `minRTT`. Observamos que latências mais baixas foram obtidas pelo subfluxo SF1 seguido por SF2 e SF3. Como pode ser visto nas figuras, na maioria dos casos, cargas de trabalho mais altas foram observadas com subfluxos que proporcionaram latências mais baixas.

Nos cenários de carga de tráfego com maiores ganhos de agregação com MPP, ou seja, com 1000 e 2000 sensores sobre os diferentes tamanhos de carga útil CoAP, a vazão média com três caminhos (MPP-3, Figura 4(b)) é maior em comparação com os mesmos casos com dois caminhos (MPP-2, Figura 4(a)). Para 1000 sensores com 4 Bytes de carga útil, houve agregação quase ideal de 6,5 Mbps no MPP-2P, e a 9 Mbps no MPP-3P. Para 2000 sensores com 64 Bytes de carga útil, de dois para três caminhos, houve um aumento de vazão agregada de 8 Mbps para 9 Mbps. Observamos que com três caminhos não se sustentou toda a carga de tráfego, uma vez que aumentar os tamanhos de carga útil CoAP impôs uma carga de trabalho maior nos subfluxos MPTCP. Maior vazão agregada foi observada em todos os cenários MPP-2P, como mostrado na Figura 4(a). Em cenários com MPP-3P, no entanto, cargas úteis maiores aumentaram a vazão agregada para a carga de até 500 sensores, enquanto o tráfego foi movido de subfluxos mais rápidos (SF1) para mais lentos (SF2 e SF3) na carga de 1000 e 2000 sensores. Como esperado, pacotes de maior carga útil também afetam negativamente o desempenho da aplicação CoAP, levando a tempos de resposta maiores e menos requisições por segundo atendidas em cargas altas. As avaliações detalhadas de desempenho podem ser encontradas nos Capítulos 4 e 5 da dissertação [Silva 2020], incluindo outros cenários e implementações de arquiteturas de escoamento de tráfego de IoT.

5. Conclusões e Trabalhos Futuros

Neste trabalho, propomos, implementamos e validamos uma nova arquitetura de comunicação, onde infraestruturas de IoT podem se beneficiar do transporte por múltiplos caminhos concorrentes durante o descarregamento de tráfego M2M da infraestrutura para um servidor remoto. Embora os benefícios de transmissões por múltiplos caminhos para

usuários finais da Internet já sejam bem conhecidos, pouco se sabia sobre os impactos dessas transmissões em ambientes de IoT. Neste trabalho, pudemos identificar e observar experimentalmente os benefícios. De fato, o nó MPP é um novo dispositivo de rede, elemento o qual mostramos ser capaz de lidar com o tráfego M2M de entrada e saída por meio de sub-fluxos MPTCP. Nossos resultados ilustram o potencial da arquitetura proposta, com MPP e a sua capacidade de transporte de caminhos múltiplos como principais habilitadores para o descarregamento eficiente de tráfego em infraestruturas de IoT. As próximas etapas possíveis serão avaliar o impacto das opções de projeto e outras implementações da arquitetura atual, por exemplo, com o protocolo MPQUIC (*MultiPath QUIC*), que é um novo protocolo de transporte rico em recursos e com maior flexibilidade para enfrentar desafios de transmissões M2M na Internet.

6. Agradecimentos

Este trabalho foi parcialmente financiado pela empresa TecSys do Brasil Industrial.

Referências

- Boccassi, L., Fayed, M. M., and Marina, M. K. (2013). Binder: A system to aggregate multiple internet gateways in community networks. In *Proceedings of the 2013 ACM MobiCom workshop on Lowest cost denominator networking for universal access*, pages 3–8.
- Hong, J., Kovatsch, M., Schooler, E., and Kutscher, D. (2020). IoT Edge Challenges and Functions, draft-hong-t2trg-iot-edge-computing-05. Internet draft, IETF.
- Keukeleire, N., Hesmans, B., and Bonaventure, O. (2019). Increasing broadband reach with hybrid access networks. *arXiv preprint arXiv:1907.04570*.
- Kovatsch, M., Lanter, M., and Shelby, Z. (2014). Californium: Scalable Cloud Services for the Internet of Things with CoAP. In *2014 International Conference on the Internet of Things (IOT)*, pages 1–6.
- Liu, X., Shan, D., Shu, R., and Zhang, T. (2018). Mptcp tunnel: an architecture for aggregating bandwidth of heterogeneous access networks. *Wireless Communications and Mobile Computing*, 2018.
- Silva, C. F. (2020). Descarregamento de tráfego de redes iot/edge por transmissões de múltiplos fluxos. Dissertação de Mestrado em Ciência da Computação, Universidade Federal de São Paulo.
- Silva, C. F., Ferlin, S., Alay, O., Brunstrom, A., and Kimura, B. Y. L. (2021). IoT Traffic Offloading with MultiPath TCP. (*to appear in*) *IEEE Communications Magazine*.
- Slabicki, M. and Grochla, K. (2016). Performance Evaluation of CoAP, SNMP and NETCONF Protocols in Fog Computing Architecture. In *2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*, pages 1315–1319.
- Song, L., Niyato, D., Han, Z., and Hossain, E. (2015). *Machine-to-machine (M2M) communications*, page 338–368. Cambridge University Press.
- Verma, P. K., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., Alsabaan, M., Khalifa, T., Abdelkader, T., and Abogharaf, A. (2016). Machine-to-machine (m2m) communications: A survey. *Journal of Network and Computer Applications*, 66:83 – 105.